UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/896,255
Filing Date: June 28, 2001
Appellant(s): HSU ET AL.

Gregory J. Koerner
Reg. No. 38,519
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2 October 2006 appealing from the Office action mailed 24 January 2006. This is an updated Examiner's Answer in response to communication filed cancelling claim 42.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

A substantially correct copy of appealed claim 42 appears on page 27 of the Appendix to the appellant's brief. The minor errors are as follows: The Appendix needs to indicate that claim 42 is cancelled as indicated on correspondence 2 December 2008.

(8) Evidence Relied Upon

6,708,273	Ober et al.	24 March 2004
6,820,203	Okaue et al.	16 November 2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-3, 5-24, and 26-42 are rejected under 35 U.S.C. 102(e) as being anticipated by Ober et al. U.S. Patent No. 6,708,273 (hereinafter '273).

Regarding claim 21, as per the first limitation of independent claim 21, **"A method for performing a data encryption operation in an electronic system, comprising: creating an encryption structure in a memory device by utilizing a processor"** is taught in '273 col. 2, lines 19-48 and col. 7, lines 23-34.

As per the second limitation, **"programming control registers with said processor to perform said data encryption operation"** is shown in '273 col. 5, lines 54-63.

As per the third limitation, **"accessing said encryption structure and said control registers with a DMA engine; and"** is disclosed in '273 col. 4, lines 46-60.

As per the fourth limitation, **"processing source data with an encryption module of said DMA engine to produce destination data, said encryption module utilizing command information from said encryption structure and control information from said control registers to perform said data encryption operation"** is taught in '273 col. 9, lines 36-67 and col. 7, line 35 through col. 8, line 43.

Regarding claim 22, **"wherein said data encryption operation includes at least one of a data encryption process and a data decryption process"** is shown in '273 col. 2, lines 32-47.

Regarding claim 23, **"wherein said memory device receives said source data from a source entity coupled to said electronic system, said memory device responsively storing said source data into a source data memory location until said encryption module requires said source data to perform said data encryption operation"** is disclosed in '273 col. 11, lines 7-43.

Regarding claim 25, **"wherein said electronic system includes a bridge device that facilitates bi-directional communications between said processor, one or more peripheral devices, said DMA engine, said encryption module, and said memory device"** is shown in '273 col. 11, lines 1-43.

Regarding 26, **"wherein said bridge device includes a processor interface for communicating with said processor, a memory interface for communicating with said memory device, and one or more peripheral interfaces for communicating with said one or more peripheral devices"** is disclosed in '273 col. 11, lines 32-43.

Regarding 27, **"wherein said encryption structure includes at least one command structure that has command information for performing said data encryption operation"** is taught in '273 in col. 6, line 66 through col. 7, line 23.

Regarding 28, **"wherein said command structure includes a starting source address, a starting destination address, a transfer-bytes total field, a next command-structure pointer, and a control status command"** is shown in '273 col. 25, lines 35-41.

Regarding 29, **"wherein said control status command includes an encryption/decryption field to indicate whether to perform one of said encryption process and said decryption process, an enabled/disabled field to indicate whether said data encryption operation is currently enabled, an interrupt field to designate whether an interrupt should occur following said data encryption operation, a last command field to indicate a final command structure in a linked list, and a transfer path identifier to indicate a source entity for said source data and a destination entity for destination data"** is disclosed in '273 in tables 1 & 2, as well as claim 1.

Regarding 30, **"wherein said encryption structure includes a series of command structures that are linked together in a linked list to thereby perform a series of data encryption operations"** is taught in '273 col. 5, line 41 through col. 6, line 33.

Regarding 31, **"wherein said DMA engine includes a state machine for controlling said data encryption operation, one or more command registers for locally storing one or more command structures from said encryption structure, said control registers, a data buffer, an encryption key register, and said encryption module"** is shown in '273 col. 5, line 41 through col. 6, line 33.

Regarding 32, **"wherein said control registers include a start register that said processor may program to start said data encryption operation, a halt/resume register that said processor may program to halt or resume said data encryption operation, a clear interrupt register that said processor may program to clear an interrupt of said data encryption operation, a link list address register that said processor may program with a physical address in said memory device of a first command structure in said encryption**

structure, and a status register that said DMA engine may program to indicate a current status of said data encryption operation" is disclosed in '273 in tables 1 & 2, as well as claim 1.

Regarding 33, **"wherein said processor initially creates said encryption structure in said memory device, said encryption structure including one or more command structures that each include command information for performing a separate data encryption operation"** is taught in '273 col. 7, lines 23-52.

Regarding 34, **"wherein said processor programs said control registers with data encryption information that is then locally available to said DMA engine for performing said data encryption operation"** is shown in '273 col. 7, lines 23-52.

Regarding 35, **"wherein said processor instructs said DMA engine to perform said data encryption operation after programming said control registers, said processor then releasing control of said data encryption operation and performing other system processing tasks for said electronic system"** is disclosed in '273 col. 7, lines 44-67.

Regarding 36, **"wherein said DMA engine copies one or more designated command structures from said encryption structure in said memory device into one or more command registers that are locally coupled to said DMA engine"** is taught in '273 col. 7, line 65 through col. 8, line 23.

Regarding 37, **"wherein said DMA engine controls said data encryption operation by referring to said control registers and said command registers"** is shown in '273 col. 11, lines 14-24.

Regarding 38, **"wherein a state machine coupled to said DMA engine transfers said source data from said memory device to a data buffer coupled to said encryption module, said encryption module responsively performing at least one of said data encryption process and said data decryption process to produce said destination data, said state machine then storing said destination data back into said memory device"** is disclosed in '273 col. 11, lines 1-24.

Regarding 39, **"wherein said DMA engine detects a completion condition while performing said data encryption operation, said DMA engine responsively notifying said processor regarding said completion condition"** is taught in '273 col. 7, lines 43-52.

Regarding 40, **"wherein said processor transfers said destination data from said memory device to a destination entity that is coupled to said electronic system"** is shown in '273 col. 7, lines 65 through col. 8, line 55.

As to independent claim 1, this claim is directed to an apparatus performing the method of claim 21 therefore it is rejected along similar rationale.

As to dependent claims 2-3 and 5-20; these claims all stand or fall with claims 1, 22, 23, and 25-40.

As to independent claim 41, this claim is directed to the apparatus for performing the method of claim 21 therefore it is rejected along similar rationale.

As to independent claim 42, this claim is directed to an apparatus for performing a data processing operation of the method of claim 21 therefore it is rejected along similar rationale.

Claims 4 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over '273 in further view of Okaue et al. U.S. Patent No. 6,820,203 (hereinafter '203). The motivation to

combine these references is to maintain security on a small circuit scale (see '273 col. 2 lines 28-48) "Accordingly, a memory card with an internal security unit may be provided with two types of registers: an accessible register for storing data to be transferred to the set in response to a command requesting the same; and a non-accessible register for storing an intermediate calculation result of the encryption process. Consequently, with two registers, the circuit scale of the security unit becomes large. This hampers the ability to increase the integration of the security unit structured as an IC chip. When the encryption process is to be performed a number of times, in order to remove a register that temporarily stores data, it is necessary to employ a plurality of encryption circuits so as to obtain all final data (encrypted data) at about the same time. Thus, in this case, the circuit scale also increases … Accordingly, an object of the present invention is to provide a security unit that allows security to be maintained in a small circuit scale. Another object of the invention is to provide a memory unit that includes a security unit with a small circuit scale".

Regarding claim 24, **"wherein said electronic system is implemented as one of an audio/visual electronic device, a consumer electronics device, a portable electronics device, and a computer device"** is taught in '203 in col. 2, lines 57-61 "The security unit is particularly useful as part of a memory unit that is attachable to a recording/reproduction device such as a digital audio recorder/player".

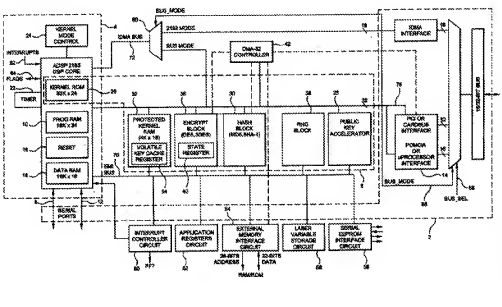
Claim 4 stands or falls with claim 24.

(10) Response to Argument

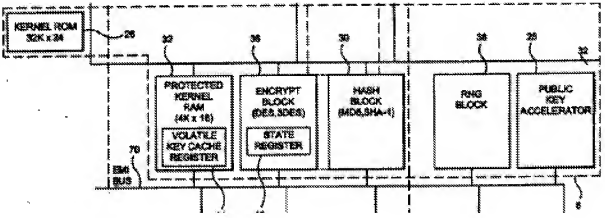
Regarding Appellant's argument first argument, on pages 7 through 8, "Ober fails to disclose: the relationship between the claimed DMA engine & encryption module".

The grounds of rejection stand, see Final Office action and Ober col. 7, line 23 through col. 8, line 43 “These commands are recognized by a microprocessor forming part of the co-processor … As mentioned previously, a standard direct memory address (DMA) controller circuit 42 is preferably included within the cryptographic co-processor”. Note Ober shows the relationship of the DMA engine and the encryption module. Also see figures 1 and 6. Note on FIG. 1, FIG. 6 is designated by the dashed line. FIG. 6 is the DMA sub-system, this is interpreted to be equivalent to the DMA engine of the claimed invention. The DMA sub-system includes encryption modules.

See FIG-1 from Ober below

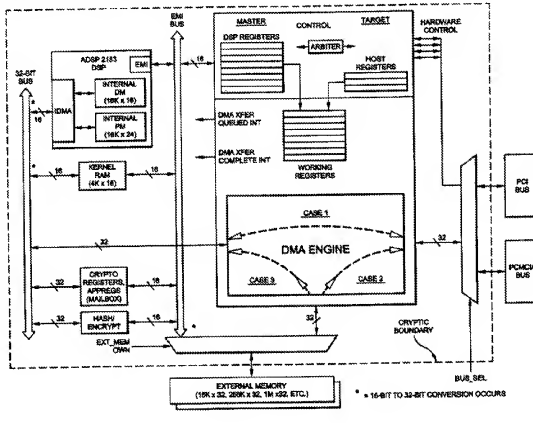


See FIG. 6 indicated above in FIG. 1, and shown below enlarged as it appears in FIG. 1



Below see FIG. 6, the DMA subsystem, notice this sub-system includes encryption and control registers.

FIG-6 32-BIT DMA SUBSYSTEM



Regarding Appellant's argument beginning on page 8, "No encryption or decryption functionality is incorporated into DMA controller circuit".

The grounds of rejection stand, specifically to understand more of Ober see col. 2, lines 18-65 "It is another object of the present invention to provide a secure communications platform that can implement a user's application and dedicate cryptographic resources to encryption and decryption requests on demand" and col. 4, lines 45-60 "Preferably, the co-processor may further include a standard direct memory access (DMA) controller circuit 42, which will be described in greater detail" and the arguments and figures shown above.

Regarding Appellant's argument on page 9, "Applicants therefore respectfully submit that Ober fails to teach a "DMA engine including an encryption module", as claimed by Applicants. On the contrary, Ober explicitly teaches a "standard direct memory access (DMA) controller circuit" without internal encryption functionality … 102 requires that every claimed limitation be identically taught by a cited reference, and becaue the Examiner fails to cite Ober to identically teach the claimed invention, Applicants respectfully request reconsideration"

The grounds of rejection stand, see above responses as well as the encryption module within the DMA sub-system. Note the DMA sub-system is equivalent to the DMA engine of the claimed invention.

Regarding Appellant's arguments on page 10 directed to claims 5 and 6, "Ober nowhere discloses a bridge device for bidirectional communication"

The grounds of rejection stand see Office action and Ober col. 11, lines 1-42 "The Application Registers also provide the mechanism which allows the DSP to arbitrate whether it

or the DMA controller (Host) has ownership of the External Memory interface" which teaches a full bus interface 'arbitrate' is interpreted to be bidirectional.

Regarding Appellant's arguments, "Furthermore Ober nowhere discloses a processor interface as well as peripherals devices".

The grounds of rejection stand see Final Office action and Ober col. 11, lines 32-43 "Primarily, the Interrupt Controller provides a new Interrupt Generation capability to the DSP or to an external Host Processor. Under programmable configuration control, a `Crypto Interrupt` may be generated due to completion of certain operations such as Encrypt Complete, Hash Complete, etc. The interrupt may be directed either at the DSP core, or provided on an output line (PF7) to a Host subsystem" note external Host or subsystems, would interpreted as peripherals.

Regarding Appellant's arguments, "in contrast to Applicants claimed command structure … the DMA registers discussed by Ober have no effect upon encryption functionalities, control pointer status".

The grounds of rejection stand see Final Action, Arguments, as well as Ober col. 25, lines 35-41 "When the DSP controls the DMA engine, it truly behaves as a general-purpose DMA controller: The DSP specifies source and destination devices/addresses and the byte count, and the DMA engine then executes the transaction. Status registers may be polled for completion, or an interrupt may be generated at the end of the transfer" and col. 31 line 53 through col. 32 line 67 "DMA Status/Configuration Register (PCISC) This 16-bit Read/Write register, as shown in the table below, allows the DSP to configure/monitor the DMA function …

The next three bits [3-5] are general status bits which indicate the busy status of the DMA engine for each of its three modes".

Regarding Appellant's arguments directed to claims 10 and 30 on pages 11 through 12, "Ober fails to disclose linked list ".

The grounds of rejection stand the portion cited shows that the algorithm selected can be a linked list see Ober col. 5, line 25 through col. 6, line 44 "The security portion of the co-processor 6 includes … It is, of course, understood that the encryption circuit 36, random number generator circuit 38, public key accelerator circuit 28, registers 34, hash circuit 30, mode control circuit 24 and other circuits used in the co-processor may be implemented by discrete components or may be equivalently formed as part of the DSP 20, which may be programmed to provide the functions of these circuits. It should also be noted that the term "circuit" used herein incorporates both hardware and software implemented connotations. The encryption circuit 36 provides a hardware assisted DES engine. A hardware assisted DES engine is provided because it is faster than a software DES engine, which would require more operations to encrypt and decrypt. The DES engine can be used to implement DES and Triple DES encryption and decryption. Furthermore, it implements four cipher modes: Electronic Code Block (ECB), Cipher Block Chaining (CBC), Cipher Feed Back (CFB), and Output Feed Back (OFB). The DES and Triple DES encrypt/decrypt operations are pipelined and preferably execute full 16-round DES in 4 clock cycles. The DES engine preferably encrypts 64 bits of data at a time and has a separate state register 40 (i.e., the feed-back or initialization vector register) that can be read and written. The state register 40 is important in allowing multiple encryption circuit contexts, thus allowing packet switching. With a writable state register 40, a previous context can be reloaded or a new

one created … A control register is provided to program the algorithm and mode to be used … A kernel mode control circuit 24 is provided for controlling a security perimeter around the cryptographic hardware and software. Because the cryptographic co-processor has a general purpose DSP and a cryptographic co-processor, the device may operate in either a user mode or a kernel mode. In the user mode the kernel space is not accessible, while in the kernel mode it is accessible. When in the kernel mode, the kernel RAM and certain registers and functions are accessible only to the secure kernel firmware. The kernel executes host requested macro level functions and then returns control to the calling application". Note this portion indicates that both can decryption and encryption can be performed in parallel execution however the design allows for selection of which algorithm to be used, which in interpreted to be equivalent to a linked list.

Regarding Appellant's arguments directed to claims 11 and 31, "Ober teaches only a "standard direct memory access (DMA) controller circuit" without any type of internal encryption functionality (see column 4, line 52). Ober therefore fails to disclose that "said DMA engine includes a state machine for controlling said data encryption operation, or more command registers for locally storing one or more command structures".

The grounds of rejection stand, See Ober figure 6 and arguments answered above.

Regarding Appellant's arguments directed to claims 12 and 32 on page 13, "claimed "control registers" … Applicants therefore respectfully request the Examiner to explicitly associate the claimed elements of claims 12 and 32 to specific teaching in Ober".

The grounds of rejection stand Status Registers are shown in Table 1, Table 2 as well as claim 1. To explicitly associate:

the 'start register' is interpreted to be equivalent to the upper and lower registers of the Host and Local address shown in Table 1 DMA &PCI Registers;

the 'halt/resume register' is interpreted to be equivalent to 'Select Delay' command in the Application Registers;

'a clear interrupt register' is interpreted to be equivalent to the 'Reset' command in columns 13-14 or the Clear selected Interrupt in col. 19 under Interrupt controller registers;

'a link list address register that said processor may program with a physical address in said memory device of a first command structure in said encryption structure' is interpreted to be equivalent to 'CGX Command register' with the 'Local Address registers' shown in Table 1, note the CGX Command in association with the Context Registers is interpreted to be equivalent to the linked list

'a current status of said data encryption operation' is indicated in Table 1, Table 2 Status Registers as well as claim 1, col. 179 lines 31-35 'status bits'.

Regarding Appellant's arguments directed to claims 13 and 33 on page 13, "Applicants submit that Ober nowhere teaches a local processor device actively creating an encryption structure for use by a DMA engine, as recited".

The grounds of rejection stand see Ober col. 5, line 40 through col. 6, line 45 "Because the cryptographic co-processor has a general purpose DSP and a cryptographic co-processor, the device may operate in either a user mode or a kernel mode. In the user mode the kernel space is not accessible, while in the kernel mode it is accessible. When in the kernel mode, the kernel

RAM and certain registers and functions are accessible only to the secure kernel firmware. The kernel executes host requested macro level functions and then returns control to the calling application" and col. 11, line 63 through col. 12, line 6 "The CryptIC is designed to allow additional Security Functions to be added to the device through a Secure Download feature. Up to 16 k words of code may be downloaded into internal memory within the DSP and this code can be given the security privileges of the Kernel firmware. All downloaded firmware is authenticated with a Digital Signature and verified with an on-chip Public Key. Additional functions could include new Encryption, Hash or Public Key algorithms such as IDEA, RC-4, RIPEMD, Elliptic Curve, etc".

Regarding Appellant's arguments, beginning on page 14 "In particular, independent claim 41 recites "means for creating an encryption structure in a memory device" … Applicants respectfully submit that, in light of the substantial differences between the teaching of Ober and Applicants' invention as disclosed".

The grounds of rejection stand, Ober teaches a means for creating an encryption structure in a memory device, see arguments presented and answered above.

Regarding Appellant's arguments, on pages 15-17, " Applicants submit that Ober in combination with Okaue fail to teach a substantial number of the claimed elements of the present invention. Furthermore, Applicants also submit that neither Ober nor Okaue contain teaching for combining the cited references to produce the Applicants' claimed invention".

The grounds of rejection stand, Ober teaches a motivation to combine the references to utilize a small memory device to maintain security. Okaue teaches the limitations of claims 4

and 24 in combination with Ober which, teaches all of the other limitations. Claims 4 and 24 implements the system taught in Ober on a portable device.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/ELLEN TRAN/
Primary Examiner, Art Unit 2433

Conferees:
Chris Revak
/Christopher Revak/
Primary Examiner, Art Group 2431

Kim Vu
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435